学術機関が発行する証明書のデジタル化における相互運用性確保に向けて

伊藤忠テクノソリューションズ株式会社
みらい研究所
貞弘　崇行

本発表のアウトライン

- 本発表の対象者とお持ち帰りいただきたいこと
- 学術機関が発行する証明書デジタル化の背景
- 学術機関が発行する証明書デジタル化の課題例
- 課題対処に対する方向性を示すリファレンスフレームワーク（仮称）
  - 概要
  - スケジュール

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

本発表の対象者とお持ち帰りいただきたいこと

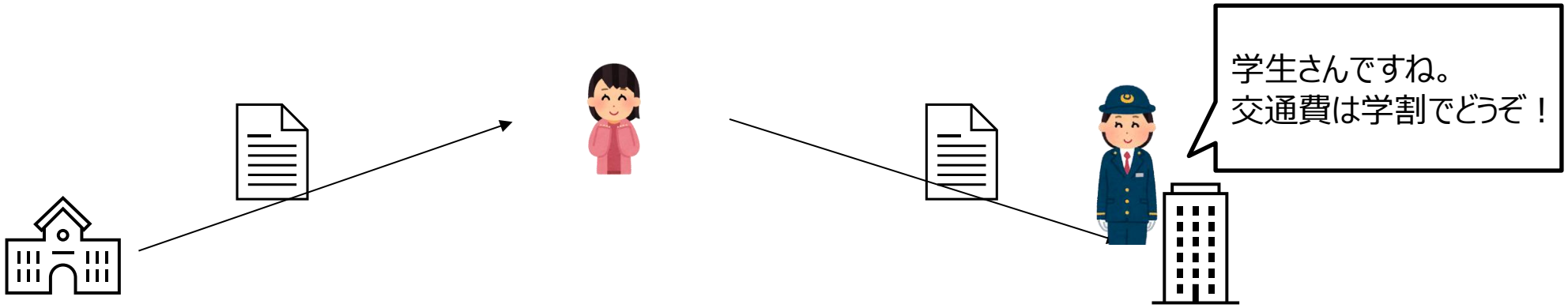
- 本発表の対象者
  - 所属
    - 大学などの学術機関（学認参加機関に限らない）に所属する方
    - 上記の機関へサービスを提供するシステムを企画・構築する組織
  - 役割
    - 学術機関におけるデジタル化された証明書を発行するシステムの導入検討者および運用者
    - 学術機関におけるデジタル化された証明書を利用し、サービスを提供するシステムの企画、設計担当者および運用者

- お持ち帰りいただきたいこと
  - 学術機関が発行する証明書のデジタル化にあたり、相互運用のためにはスキーマや利用プロトコル、ガバナンスの標準化が必要であることの理解
  - NIIにて実施している共同研究の結果としてまとめる予定の、そうした標準の方向性を示すリファレンスフレームワーク（仮称）取組の概要とそのスケジュール

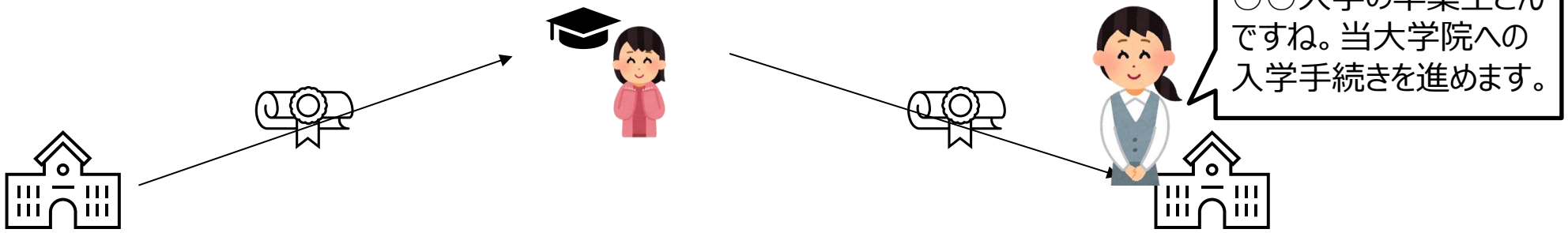
© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

学術機関が発行する証明書の利用例

- 在学証明書を使って、学割サービスを利用



- 卒業証明書を使って、大学院への入学手続きを実施



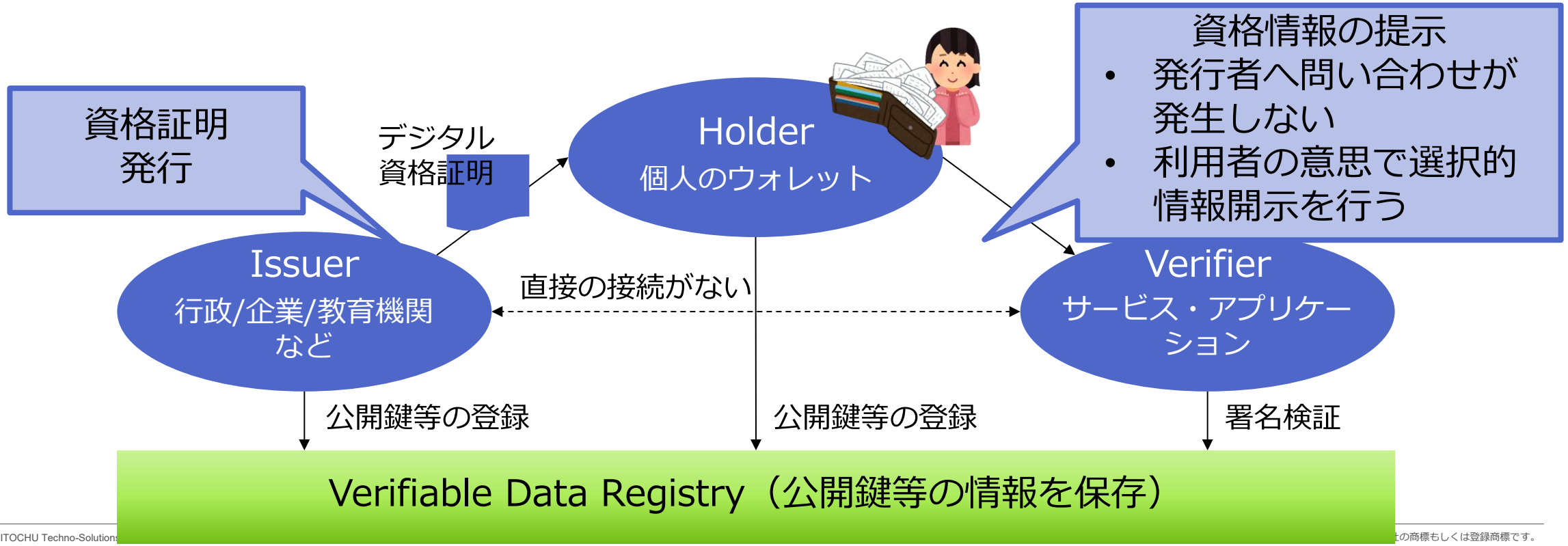
© 2022 ITOCHU Techno-Solutions Corporation

記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

デジタル化された資格証明実現に適したIHVモデル

検証可能性と制御可能性の両立

- 資格証明の発行と提示を分離、プライバシーと可用性の確保
- 公開鍵暗号などによるデータの真正性の担保



© 2022 ITOCHU Techno-Solutions
社の商標もしくは登録商標です。

IHVモデルが他の学術機関でも採用されつつある例

- InCommon（米国の学術フェデレーション）ではIHVモデルにより、学術資格、研究コンピューティング、金融、医療、政府など、複数の産業分野でのコラボレーションが広がる可能性があると想定
  Key Identity Trends in Research & Education: AI, Federation, and Trust Management – InCommon

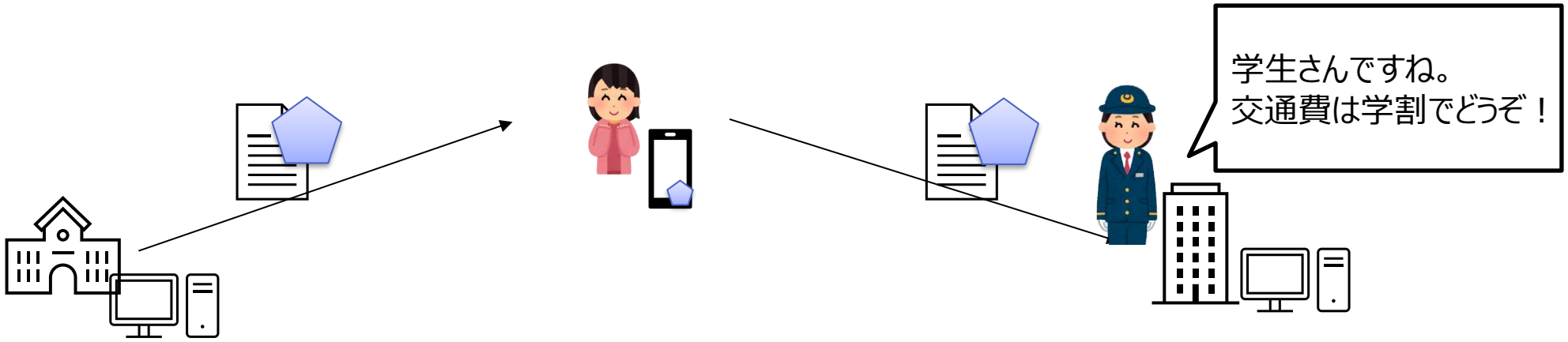
- 欧州デジタルアイデンティティウォレットにおいては、IHVモデルを利用して学生の移動性を向上させ、資格確認を簡素化し、欧州連合全体で生涯学習を支援することを目的とした大規模パイロットプロジェクトであるDC4EUを実施中
  Digital credentials in education - DC4EU

- MITを中心として組成されたDCC（Digital Credential Consortium）では、学位や職業上の資格、オンラインコースで取得した資格の発行、保存、表示、検証を行うための信頼性があり分散型のインフラを構築する取組を実施中
  Digital Credentials Consortium

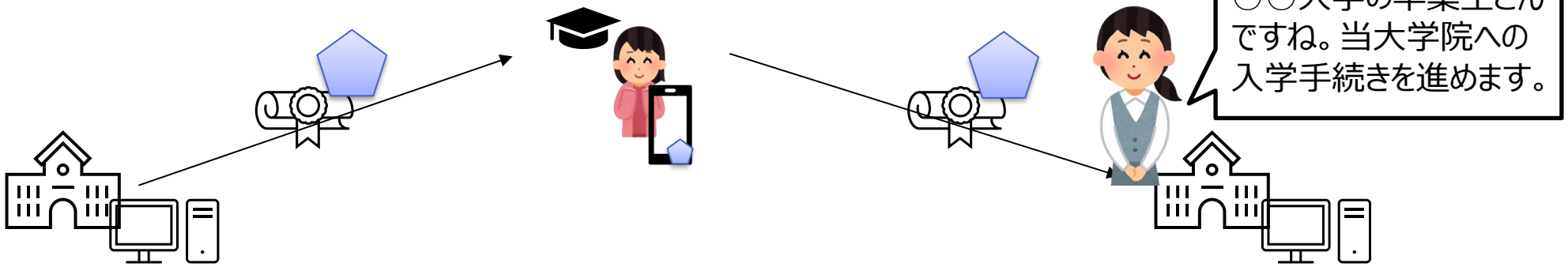
© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

学術機関が発行する証明書のデジタル化利用例

- 在学証明書を使って、学割サービスを利用



- 卒業証明書を使って、大学院への入学手続きを実施

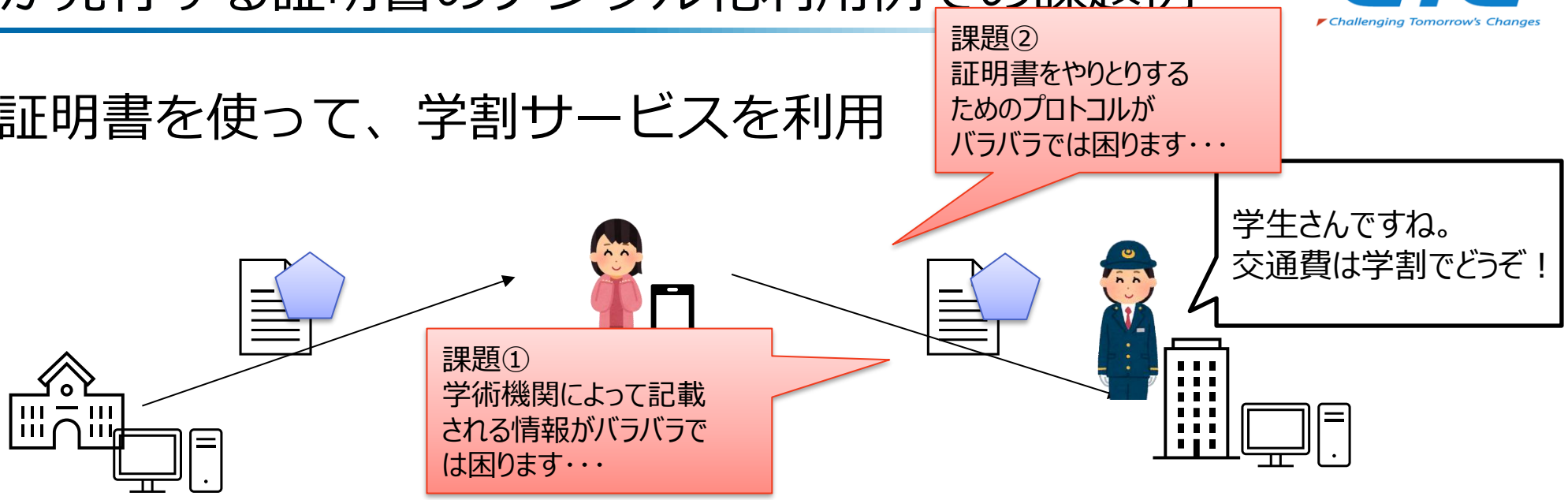


© 2022 ITOCHU Techno-Solutions Corporation

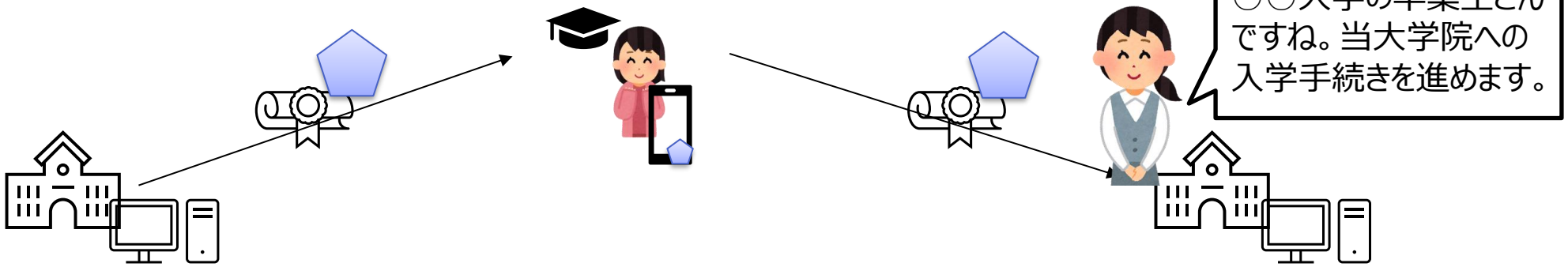
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

学術機関が発行する証明書のデジタル化利用例での課題例

- 在学証明書を使って、学割サービスを利用



- 卒業証明書を使って、大学院への入学手続きを実施



© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

相互運用性の確保のために

- スキーマやトランスポートプロトコルの標準化
  - 前頁課題①や②
  - 課題①については標準スキーマ策定の取組が進行中
    - 学術機関の発行する証明書のための標準属性とその利用シーン
  - 課題②についてはISO 18013-5/7（mDL）やOID4VCsとして標準化されつつある

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

相互運用性の確保のために

- スキーマやトランスポートプロトコルの標準化
  - 前頁課題①や②
  - 課題①については標準スキーマ策定の取組が進行中
    - 学術機関の発行する証明書のための標準属性とその利用シーン
  - 課題②についてはISO 18013-5/7（mDL）やOID4VCsとして標準化されつつある

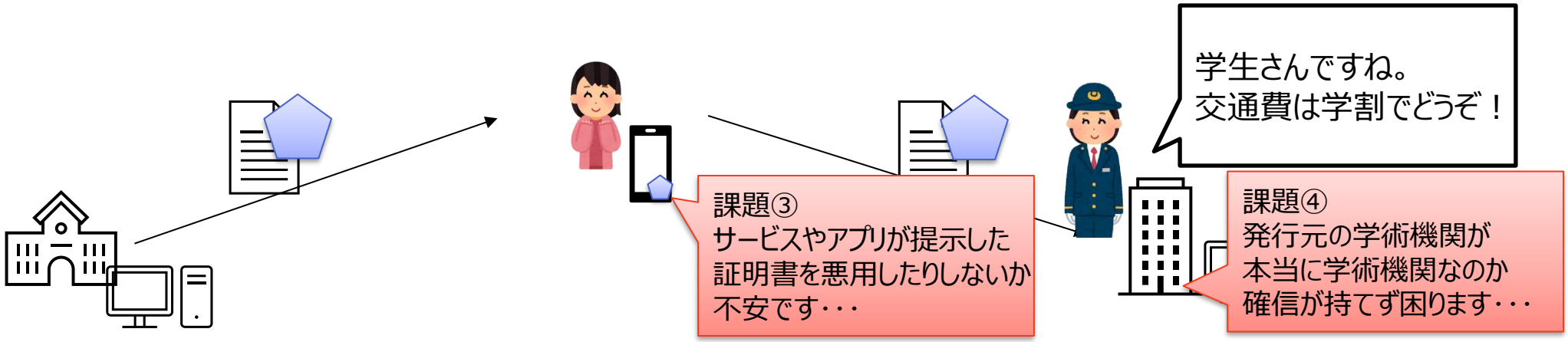
に加えて

- ガバナンスの確保
  - 証明書の発行者や利用先のサービスは信頼できるのか
  - 証明書を格納するウォレットは信頼できるのか
  - 証明書の対象者と提示者が一致することをどう確認するのか　など

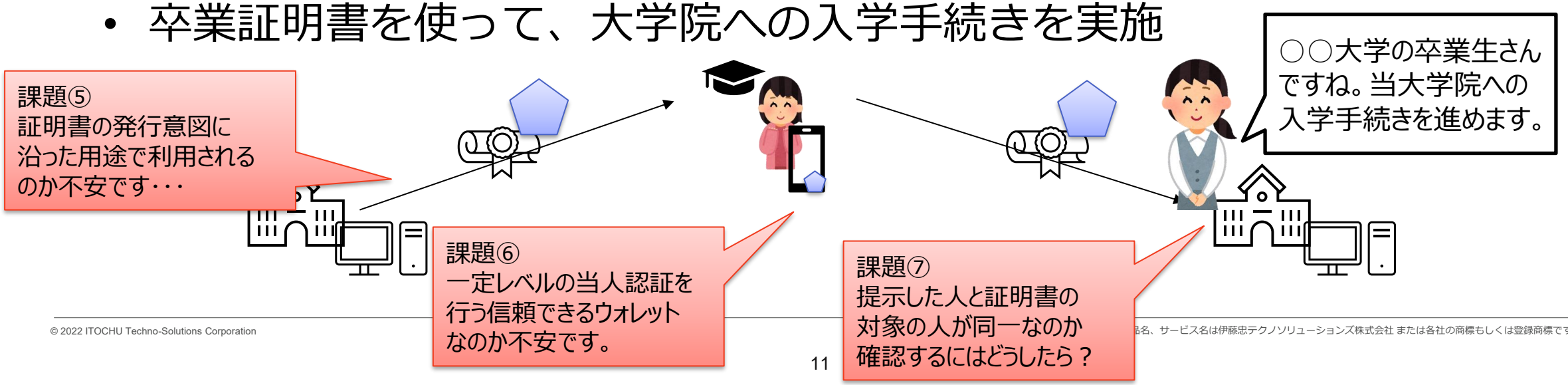
© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

学術機関が発行する証明書のデジタル化利用例での課題例

- 在学証明書を使って、学割サービスを利用



- 卒業証明書を使って、大学院への入学手続きを実施



© 2022 ITOCHU Techno-Solutions Corporation
品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

リファレンスフレームワーク（仮称）の内容 #1

- 目的
  - 学術機関が発行する各種資格証明を安全に相互運用するために必要なガバナンスや技術仕様標準の策定
  - 上記を支えるための以下の策定
    - 資格証明の発行機関である発行機関である各学術機関が資格情報を発行する際に付与する各機関のデジタル署名、各機関がトラストフレームワークにより認定されている機関であることを証明する認定機関のデジタル署名のそれぞれについて、受け取り側の機関が検証可能なアーキテクチャ
    - 各参加機関の位置づけと遵守事項

- スコープ
  - 本書は学術機関が発行するデジタル化された証明書を対象とする。
    - 学術機関が発行する証明書は受け取り側によっては一部対象となった人の身分証明に使われることもあるが、学術機関として証明しているのは資格である。
    - 身分証明として使われる場合については本書の対象外とする。なぜなら、提示された資格証明の対象者と提示者が一致することの確認が必要となるが、これは必ずしも学術機関が保証できるとは限らないため。
  - 本書が対象とする上述証明書の流通範囲は日本国内学術機関間およびその提供を受ける民間企業とする。

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

リファレンスフレームワーク（仮称）の内容 #2-1

- 対象読者
  - 所属機関
    - 大学、短期大学、高等専門学校、大学共同利用機関、国公立試験研究機関並びに研究又は研究支援を目的とする独立行政法人および特殊法人
    - 上記の機関へサービスを提供するシステムを企画・構築する機関、又はその部門
    - 上述機関は学認参加機関のみに限るものではない
  - 役割
    - 学術機関におけるデジタル化された証明書を発行するシステムの導入検討者および運用者
    - 学術機関におけるデジタル化された証明書を利用し、サービスを提供するシステムの企画、設計担当者および運用者
  - 利用シーン
    - 学術機関における資格証明を発行するシステム導入において、設計および運用を検討する際に参照するリファレンスとして利用。
    - 学術機関における資格証明を利用するサービスを提供するシステム設計および運用を検討する際に参照するリファレンスとして利用。

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

リファレンスフレームワーク（仮称）の内容 #2-2

- 対象読者
  - （続き）
  - 技術レベル
    - IHVモデルの理解
    - OID4VC, ISO 18013-5/7などの概要理解
  - 読み手に期待すること
    - 学術機関が発行する各種資格証明を発行、格納、利用するシステムを構築する際には、本フレームワークに記載された遵守事項を踏まえた企画、設計、構築を進めること

- 位置付け
  - Normativeドキュメント（学認運用基準）の拡張に向けたインプット文書
  - 学認トラストフレームワークのブラッシュアップも進む想定

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

リファレンスフレームワーク（仮称）の目次構成 #1

1. はじめに
    a. 背景
    b. 本書の目的
    c. 対象範囲
    d. 想定するユースケース
    e. 対象とするデジタルクレデンシャル
    f. 対象読者
    g. 用語定義
2. 全体像
    a. アーキテクチャー
    b. 各アクター
    c. 現在の学認トラストフレームワークとデジタルクレデンシャル発行の差分と考慮事項
3. ガバナンスと認定
    a. マネジメントシステム全体像
    b. アクターごとの責任範囲
    c. 認定スキーム

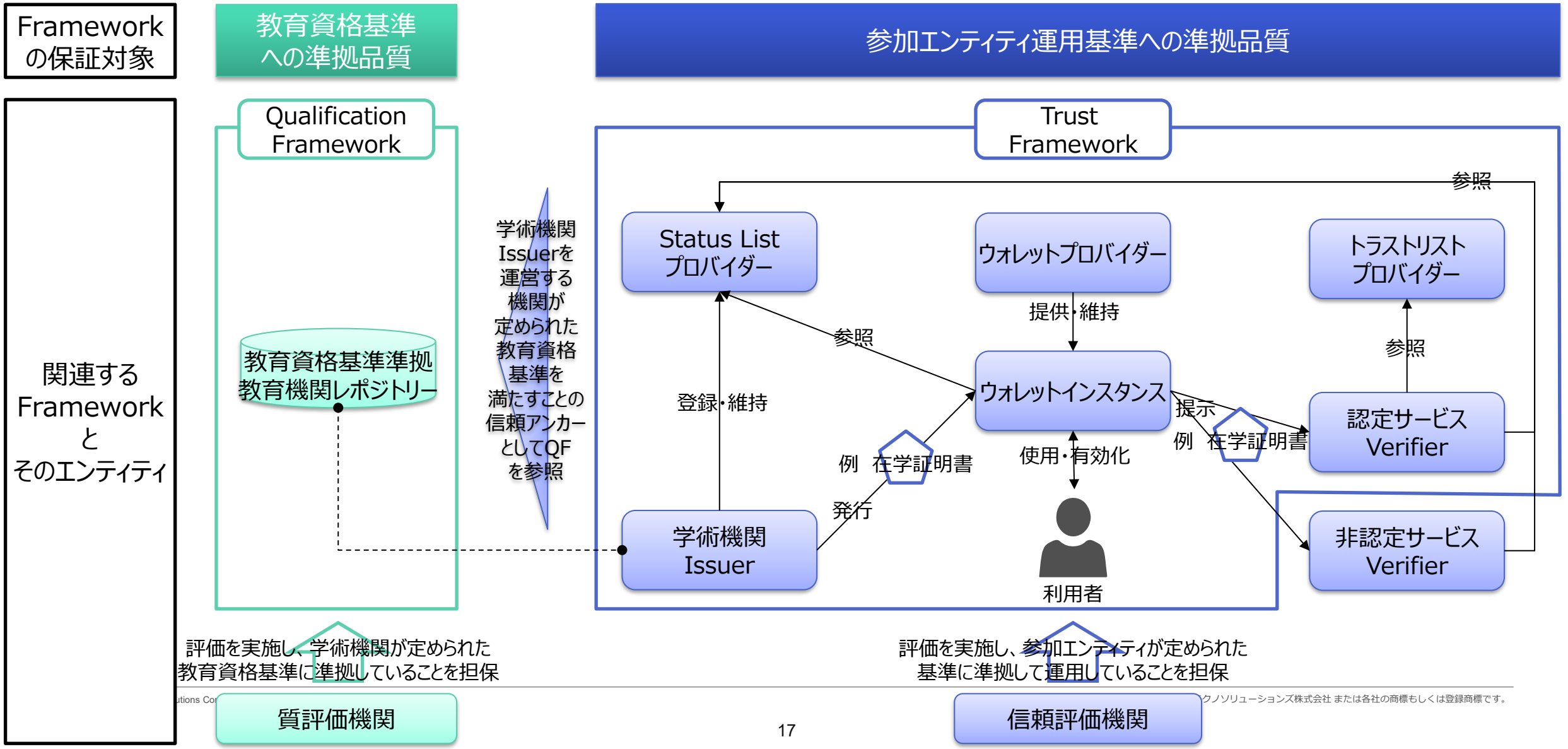
© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

リファレンスフレームワーク（仮称）の目次構成 #2

4. データフォーマットとトランスポートプロトコル
    a. データフォーマットとしてSD-JWT VC、mDL/ISO 18013-5/7
    b. トランスポートプロトコルとしてOID4VCs、mDL/ISO 18013-5/7
    c. スキーマ（？付属表？）
5. 各ライフサイクルにおける遵守事項
    a. ウォレットソリューションライフサイクル
        a. ウォレットソリューション登録時、廃止時
    b. ウォレットライフサイクル
        a. ウォレットインストール時、ウォレットに脆弱性発覚時、など
    c. Issuerライフサイクル
        a. Issuer新設時、廃止時
    d. Verifierライフサイクル
        a. Verifier新設時、廃止時
    e. クレデンシャルライフサイクル
        a. 発行時、クレデンシャルに含まれる情報更新時、失効時、など
6. 実装者向けガイド
7. 参考情報（海外事例）

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

アーキテクチャーとエンティティ（案） #1



クノソリューションズ株式会社 または各社の商標もしくは登録商標です。

アーキテクチャーとエンティティ（案） #2

エンティティ	エンティティが担う責任（赤字部は現行学認モデルエンティティからの差分）
学術機関Issuer	1. 当人認証 2. アイデンティティ情報の収集と管理 3. ウォレットインスタンスの情報保持と管理
ウォレットプロバイダー	1. ウォレットインスタンスの配布と管理
ウォレットインスタンス	1. デジタル化された証明書の管理 2. デジタル化された証明書の提示
サービスVerifier	1. 提示されたデジタル化された証明書の検証 2. 提示されたデジタル化された証明書に応じたサービスの提供 3. 提示されたデジタル化された証明書に記載された情報の適切な保持/管理
Status Listプロバイダー	1. 発行されたデジタル化された証明書の状態管理
トラストリストプロバイダー	1. 学術機関Issuerや認定されたサービスVerifier、ウォレットプロバイダー、Status Listプロバイダーの管理
信頼評価機関	1. 学術機関Issuerや各種サービスVerifier、ウォレットプロバイダー、Status Listプロバイダー、トラストリストプロバイダーが遵守すべき運用基準の明示 2. 上述の基準を満たしていることの認定

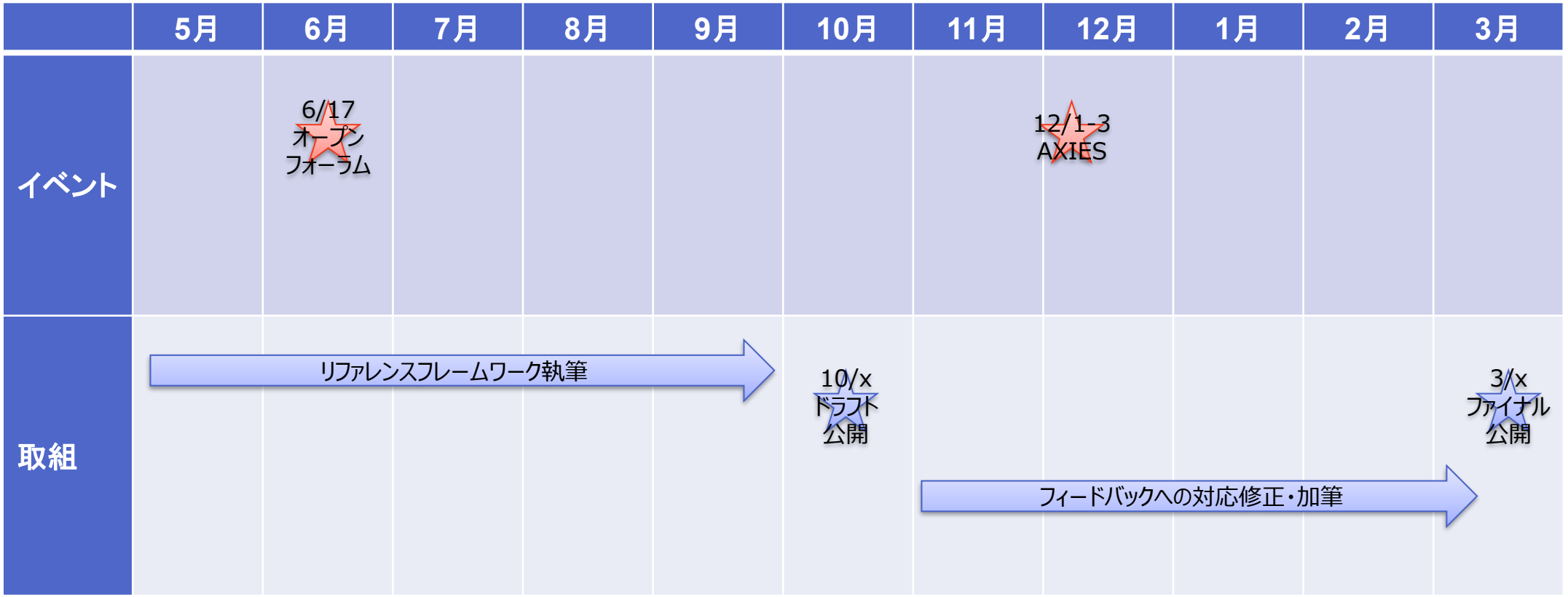
© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

アーキテクチャーとエンティティ（案） #3

エンティティ	エンティティが担う責任（赤字部は現行学認モデルエンティティからの差分）
質保証機関	1. 設置認可および認証評価などの制度に基づいた高等教育機関認定の実施 2. 認定された機関の、日本の教育資格枠組みにおけるレベルの保証

© 2022 ITOCHU Techno-Solutions Corporation
記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

取組スケジュール

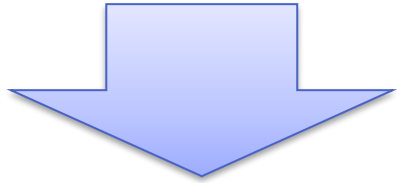


© 2022 ITOCHU Techno-Solutions Corporation

記載されている会社名、製品名、サービス名は伊藤忠テクノソリューションズ株式会社 または各社の商標もしくは登録商標です。

まとめ

- 学術機関が発行する証明書をデジタル化して流通させるためには相互運用性が必要
- 相互運用性には、利用すべきフォーマットやプロトコル標準の定義だけでなく、ガバナンスの確保も必要
- ガバナンスの確保には、学術機関IssuerやVerifier側で遵守すべき事項の明示とその遵守が必要



リファレンスフレームワーク（仮称）の策定と並行し、デジタル化された証明書の相互運用性を確保するために、意見や情報を交換する場の組成を検討します。

是非議論にご参加ください。

（ご興味をお持ちの方は以下よりお問い合わせください）

お問い合わせ | 国立情報学研究所 トラスト・デジタルID基盤研究開発センター

© 2022 ITOCHU Tec